УДК 16.776:004.58

Войтович О.П.
Волинець В.В.

ЗАСТОСУВАННЯ НЕЧІТКОЇ ЛОГІКИ ДЛЯ ОЦІНКИ РИЗИКІВ У СИСТЕМІ АДАПТИВНОГО АУДИТУ КІБЕРБЕЗПЕКИ

Вінницький національний технічний університет

Анотація

У тезах обґрунтовано доцільність інтеграції математичного апарату нечіткої логіки (Fuzzy Logic) у процедури оцінювання ризиків систем адаптивного аудиту кібербезпеки. Доведено, що перехід від бінарних моделей до нечітких дозволяє ефективно оперувати невизначеністю в умовах гетерогенних загроз. Запропоновано удосконалену модель, що трансформує вхідні параметри (рівень загрози, критичність активу, вразливості) у лінгвістичні змінні для обчислення динамічного інтегрального показника ризику. На основі аналізу сучасних досліджень (2023–2025 рр.) показано, що використання баз знань із продукційними правилами та нейро-нечітких мереж (ANFIS) забезпечує точність виявлення аномалій до 99.2% та суттєво знижує рівень хибних спрацьовувань. Результати підтверджують ефективність імплементації даного підходу в контексті міжнародних стандартів ISO/IEC 27001 та NIST CSF для підвищення резильєнтності критичної інфраструктури.

Ключові слова: *нечітка логіка; кібербезпека; адаптивний аудит; оцінка кіберризиків; нечітке оцінювання; Fuzzy Logic; функції належності; ANFIS; ISO/IEC 27001.*

Abstract

The theses substantiate the integration of fuzzy logic mathematical tools into risk assessment procedures within adaptive cybersecurity audit systems. It is proven that shifting from binary models to fuzzy ones allows effective handling of uncertainty amidst heterogeneous threats. An improved model is proposed that transforms input parameters (threat level, asset criticality, vulnerabilities) into linguistic variables to calculate a dynamic integral risk indicator. Based on an analysis of recent studies (2023–2025), it is demonstrated that using knowledge bases with production rules and neuro-fuzzy networks (ANFIS) ensures anomaly detection accuracy up to 99.2% and significantly reduces false positives. The results confirm the efficacy of implementing this approach within ISO/IEC 27001 and NIST CSF frameworks to enhance critical infrastructure resilience.

Keywords: *information security audit; cyber audit; security standards; ISO/IEC 27001; NIST CSF; fuzzy logic; risk assessment.*

Вступ

Сучасна парадигма аудиту кібербезпеки перебуває у стані фундаментальної трансформації, зумовленої експоненційним зростанням складності інформаційних систем. Традиційні методології, що спираються на дискретну булеву логіку («безпечно/небезпечно», 0/1), виявляють свою недостатню ефективність в умовах гібридної війни та складних цільових атак (APT). Проблема полягає в тому, що класифікація ситуації лише як допустимої чи критичної не враховує ступеневу природу ризику та контекстуальну невизначеність. Наприклад, наявність вразливості є фактом, але реальна небезпека залежить від нечітких факторів: кваліфікації зловмисника, привабливості активу та наявності компенсуючих контролів [1].

Подолання цих обмежень стає можливим завдяки застосуванню математичного апарату нечіткої логіки (Fuzzy Logic), запропонованого Лотфі Заде [1]. Використання функцій належності (membership functions) дозволяє оцінювати стан безпеки будь-яким значенням у безперервному діапазоні [0;1], що забезпечує необхідну гранулярність для пріоритезації ризиків [2]. Особливої актуальності цей підхід набуває в системах адаптивного аудиту (Continuous Audit), де система управління ризиками має постійно оновлювати оцінки на основі нових даних, забезпечуючи математично обґрунтовану базу для прийняття рішень щодо реагування на інциденти [3].

Результати дослідження

Проведене дослідження дозволило сформувати цілісну модель адаптивного оцінювання ризиків, яка базується на фазифікації чотирьох ключових векторів: вразливість, загроза, ймовірність та вплив. Такий підхід дозволяє структурувати оцінку ієрархічно: фактори намірів та можливостей зловмисника визначають рівень загрози, який співставляється з наявними вразливостями для визначення ймовірності успішної атаки, і, нарешті, з урахуванням потенційних збитків формується інтегральний показник ризику. Кожна змінна трансформується у лінгвістичні терми (наприклад, «низький», «середній», «високий») за допомогою трикутних або трапецієподібних функцій належності. Це дозволяє системі враховувати неоднозначність даних, коли, наприклад, рівень загрози одночасно має ознаки «середнього» та «високого» з різними ступенями відповідності [4]. Водночас, застосування інтервальних нечітких множин типу-2 (Type-2 Fuzzy Sets) дозволяє додатково підвищити адекватність оцінювання станів критичних систем в умовах недовизначених вхідних даних, надаючи експертам інтервальний вихід для прийняття більш зважених рішень [5].

Фундаментальною складовою розробленої архітектури є база знань, сформована з нечітких правил продукційного типу: IF (умова) THEN (висновок). Глибинний аналіз роботи [6] дозволив визначити критичні вагові коефіцієнти для оцінки ймовірності реалізації загрози в системах IIoT: привабливість активу (вага 0.4126), існуючі заходи контролю (вага 0.3952) та історія попередніх інцидентів (вага 0.1929). Використання цих точних значень у базі зі 125 правил дозволяє системі аудиту імітувати міркування досвідченого експерта, який інтуїтивно розуміє, що цінний актив навіть із середнім захистом атакуватимуть частіше, ніж малоцінний.

Результати дослідження [8] також демонструють високу ефективність нечіткої логіки у задачах виявлення вторгнень (IDS), що є невід'ємною частиною технічного аудиту. Робота [7] показала, що використання нечіткої моделі, яка аналізує 38 параметрів телеметрії мережевого трафіку, забезпечує підвищення точності виявлення поліморфних атак на ~10% порівняно з традиційними методами. Більше того, новітні дослідження підтверджують, що такі системи досягають точності 99.2% при рівні хибних спрацьовувань 0.008, що є критичним показником для зменшення навантаження на аналітиків SOC і запобігання «втомі від сповіщень» [8].

В контексті управління доступом (Access Control), який є ключовим об'єктом аудиту відповідності, нечітка логіка дозволяє реалізувати концепцію адаптивного ризик-орієнтованого контролю. Дослідження [9] пропонує модель, де рішення про надання доступу динамічно обчислюється на основі контексту (час, локація, історія ризиків). Це дозволяє аудиторам перевіряти не просто наявність статичних прав, а коректність роботи алгоритмів прийняття рішень, що значно підвищує рівень реальної безпеки.

Окремий пласт результатів стосується застосування нечіткої логіки для оцінки відповідності стандартам ISO/IEC 27001. Розробки у сфері нечітких експертних систем дозволяють оцінювати ступінь зрілості процесів не бінарно («виконано/не виконано»), а гранулярно (наприклад, «впроваджено на 60%»), агрегуючи оцінки по сотням контролів у єдиний показник [2]. Також перспективним є використання нейро-нечітких систем (ANFIS), які забезпечують автоматичне налаштування функцій належності, надаючи системі аудиту здатність до самонавчання [8].

Висновок

Впровадження нечіткої логіки в методологію аудиту кібербезпеки є критичною умовою переходу до адаптивного управління ризиками. Це дозволяє вирішити проблему втрати інформації, властиву бінарним методам, та забезпечує об'єктивну кількісну оцінку завдяки використанню зважених правил в умовах невизначеності.

Доведена ефективність нечітких моделей у виявленні вторгнень (точність понад 99%) та їх сумісність зі стандартами ISO/IEC 27001 трансформує аудит з інструменту фіксації порушень у механізм проактивного реагування. Перспективним є подальше поєднання цього підходу з генеративним ШІ для створення автономних систем безперервного моніторингу.

СПИСОК ВИКОРИСТАННОЇ ЛІТЕРАТУРИ

1. Wong, C. T. (2022). Fuzzy logic and decision-making: A paradigm shift in risk management. *International Journal of Education and Science Research Review, 9*(2). https://ijesrr.org/publication/82/25.%20ijesrr%20march%202022.pdf
2. Kozhakhmet, K., Bortsova, G., Inoue, A., & Atymtayeva, L. (2012). Expert system for security audit using fuzzy logic. In *Proceedings of the Twenty-Third Midwest Artificial Intelligence and Cognitive Science Conference (MAICS 2012)* (Vol. 841, pp. 146–151). CEUR Workshop Proceedings. https://ceur-ws.org/Vol-841/submission_35.pdf
3. Garcia, J. M. S. (2025). Nonlinear threats and adaptive defenses: A complexity perspective on cybersecurity challenges. *International Multidisciplinary Journal of Research for Innovation, Sustainability, and Excellence (IMJRISE), 2*(6), 75–81. https://doi.org/10.5281/zenodo.15575481
4. Rezaei, M., & Borjalilu, N. (2018). A dynamic risk assessment modeling based on fuzzy ANP for safety management systems. *Aviation, 22*(4), 143–155. https://doi.org/10.3846/aviation.2018.6983
5. Баришев, Ю., Кондратенко, Н., Казміревський, В., & Кирилащук, Т. (2023). Нечіткі множини типу-2 в задачах моделювання та оцінювання станів критичних систем з недовизначеними вхідними даними та використанням експертів. *Інформаційні технології та комп'ютерна інженерія, 57*(2), 13–24. https://doi.org/10.31649/1999-9941-2023-57-2-13-24
6. Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., Makhazhanova, U., Adalbek, A., Taberkhan, R., Zakirova, A., & Salykbayeva, A. (2023). Fuzzy logic and its application in the assessment of information security risk of industrial Internet of Things. *Symmetry, 15*(10), Article 1958. https://doi.org/10.3390/sym15101958
7. Subach, I., Fesokha, V., Mykytiuk, A., Kubrak, V., & Korotayev, S. (2021). Simulation model of a fuzzy cyber attack detection system. In *Selected Papers of the XXI International Scientific and Practical Conference "Information Technologies and Security" (ITS 2021)* (Vol. 3241, pp. 92–101). CEUR Workshop Proceedings. https://ceur-ws.org/Vol-3241/paper9.pdf
8. Iantorno, M. S., & Beladda, K. (2025). Fuzzy logic for cybersecurity: Intrusion detection and privacy preservation with synthetic data. In *Proceedings of the 17th International Conference on Agents and Artificial Intelligence* (Vol. 3, pp. 376–382). SCITEPRESS – Science and Technology Publications. https://doi.org/10.5220/0013137300003890
9. Atlam, H. F., Walters, R., Wills, G., & Daniel, J. (2019). Risk estimation using fuzzy logic in the Internet of Things. *Mobile Networks and Applications*. Advance online publication. https://doi.org/10.1007/s11036-019-01214-w

Волинець Віталій Володимирович — аспірант групи 125-24а, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: volynets1026@gmail.com

Войтович Олеся Петрівна — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail voytovych.vk.vntu.edu.ua

Volynets Vitalii V. — Faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: volynets1026@gmail.com

Voytovych Olesya P. — Ph.D., Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail voytovych.vk.vntu.edu.ua